REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

Public Reporting Burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comment regarding this burden estimate or any other aspect of this collection of information, including suggesstions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington DC 20503

1. AGENCY USE ONLY (Leave Blank)

2. REPORT DATE:
22-Jun-2007

3. REPORT TYPE AND DATES COVERED
Final Report 1-Apr-2002 - 31-Dec-2006

4. TITLE AND SUBTITLE
Complexity Bounds for Quantum Computation

5. FUNDING NUMBERS
DAAD19-02-1-0058

6. AUTHORS
Steven Homer

8. PERFORMING ORGANIZATION REPORT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Boston University
Office of Sponsored Programs
Trustees of Boston University
Boston, MA 02215 -

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
43392-PH-QC.5

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
The abstract is below since many authors do not follow the 200 word limit

14. SUBJECT TERMS
final report, quantum complexity, quantum circuits

15. NUMBER OF PAGES
Unknown due to possible attachments

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
UNCLASSIFIED

18. SECURITY CLASSIFICATION ON THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
UL

Report Title

Final Report for DAAD19-02-1-0058

Complexity Bounds for Quantum Comp[utation

ABSTRACT

This project focused on upper and lower bounds for quantum computability using constant depth quantum circuits, and on the complexity theory of such circuits. It established significant differences between resource bounded quantum and classical computation models, particularly emphasizing new examples of where quantum circuits are more powerful than their classical counterparts.

A second focus and outgrowth of this work was the creation of efficient quantum algorithms for specific problems and central combinatorial functions. Recent finding include upper bounds for the computational power of constant depth circuits composed of single qubit and CNOT gates, and lower bounds for the computational power of constant depth circuits with single qubit, CNOT and fanout gates. These results represent the power and the limits of small, possibly realizable quantum circuits.

Also examined were bounds on computations with additional storage qubits (ancillae), and natural simple functions (realized by smaill depth circuits) which require ancillae for their computation.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

F. Green, A. Roy, and H. Straubing, Bounds on an exponential sum arising in Boolean circuit c\omplexity, in Comptes Rendus 341(5) (2005), pp. 279-282.

M. Fang, S. Fenner, F. Green, S. Homer, and Y. Zhang, Quantum lower bounds for fanout, arXiv \preprint quant-ph/0312208. In Quantum Information and Computation 6 (2006), pp. 46-57.

F. Green, The Correlation Between Parity and Quadratic Polynomials Mod 3, in 17th Annual IEEE\ Conference on Computational Complexity, IEEE Computer Society Press (2002), pp. 65 -72. Appe\ared in Journal of Computer and System Sciences 69 (2004) pp. 28 - 44.

F. Green, S. Homer, and C. Pollett, On the complexity of quantum ACC, Boston University CS De\pt. preprint BUCS-TR-2000-003, and in arXiv.org, report quant-ph/0002057. In 15th Annual IEEE\ Conference on Computational Complexity, IEEE Computer Society Press, (2000), pp. 250 - 262. \Combined/expanded version with authors F. Green, S. Homer, C. Moore, and C. Pollett, under th\e title "Counting, fanout and the complexity of quantum ACC," appeared in Quantum Information\ and Computation 2 (2002), pp. 35 - 65.

F. Green and R. Pruim, Relativized separation of EQP from P(NP), in Information Processing Le\tters, 80 (2001) pp. 257 - 260.

Number of Papers published in peer-reviewed journals: 5.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

D. Bera, F. Green, and S. Homer,
Sigact News, June 2007. vol 38, no 2, pages 35-50.

S. Homer, and L. Fortnow,
A Brief History of Complexity Theory,
Bulletin of the European Association for
Theoretical Computer Science (80), June 2003, pages 95-133.
Presented at IEEE Conf. On Complexity Theory,
Montreal, May, 2002.

Number of Papers published in non peer-reviewed journals: 2.00

(c) Presentations

Number of Presentations: 7.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

Peer-Reviewed Conference Proceeding publications (other than abstracts):

S. Fenner, F. Green, S. Homer, and Y. Zhang, Bounds on the power of constant-depth quantum ci\rcuits, arXiv preprint quant-ph/0312209. Appeared in Proceedings of Fundamentals of Computati\on Theory: 15th International Symposium, Lecture Notes in Computer Science 3623 (2005), pp. 4\4-55.

F. Green, The Correlation Between Parity and Quadratic Polynomials Mod 3, in 17th Annual IEEE\ Conference on Computational Complexity, IEEE Computer Society Press (2002), pp. 65 -72. Appe\ared in Journal of Computer and System Sciences 69 (2004) pp. 28 - 44.

F. Green, S. Homer, and C. Pollett, On the complexity of quantum ACC, Boston University CS De\pt. preprint BUCS-TR-2000-003, and in arXiv.org, report quant-ph/0002057. In 15th Annual IEEE\ Conference on Computational Complexity, IEEE Computer Society Press, (2000), pp. 250 - 262.

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 3

(d) Manuscripts

Number of Manuscripts: 3.00

Number of Inventions:

Graduate Students

NAME	PERCENT_SUPPORTED
Debajyoti Bera	0.75
Benjamin Hescott	0.10
FTE Equivalent:	**0.85**
Total Number:	**2**

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Steven Homer	0.22	No
Frederic Green	0.22	No
FTE Equivalent:	**0.44**	
Total Number:	**2**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 1.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 1.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:...... 1.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):...... 1.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 1.00

Names of Personnel receiving masters degrees

NAME	
Maosen Fang	
Natalia Luckyanova	
Total Number:	**2**

Names of personnel receiving PHDs

NAME	
Benjamin Hescott	
Total Number:	**1**

Names of other research staff

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress and Accomplishments
Final Report
Reporting Period: 4/1/2002 - 12/31/2006

Complexity Bounds for Quantum Computation
DAAD19-02-1-0058

Our project focussed on fundamental theoretical issues in quantum complexity theory and algorithms. It studied problems from the Theory Component of the Quantum Computing Roadmap. The research on complexity bears on the efficiency of quantum circuits and of simple resource bounded circuit classes. This work also impacts quantum algorithms as we are designing small circuits which can be used to implement and to improve the efficiency of fundamental quantum computations.

During the duration of this grant progress was made on several different key areas of our research program. These include research on constant depth quantum circuits, on the fanout problem for these circuits, on algorithms which simulate fundamental gates and circuit elements, and on relationships between quantum complexity classes. Research in each of these areas is described below. In the last period of this grant, comprising a 5 month no-cost extension, a few final results were established and a survey paper summarizing much of the more recent, central work on this project was written and published.

Major results obtained with the support provided for this project include:

1. The construction of minimal size and depth quantum circuits which can compute important combinatorial functions. Among these are,
   - construction of circuits computing parity, and other mod functions. These are built with small circuits composed only of Toffoli, single-qubit and Hadamard gates,
   - construction of threshold functions can be similarly composed, proving that integer division can be done with these circuits more efficiently than in classical computation,
   - construction of small circuits which can carry out phase estimation, showing that the quantum content of strong quantum algorithms like Shor's algorithm can be done with smaller and simpler circuits than had previously been thought possible.
2. Proofs of lower bounds on the capabilities of small depth quantum circuits with limited gate types to compute more complex quantum transforms. In particular, we focussed on lower bounds for

- computing parity or fanout using constant or log depth quantum circuits,
- quantum simulations of classical circuit elements and classes, such as threshold and mod functions, and
- the general relationships between quantum complexity classes and corresponding classical classes, and in particular, hierarchy theorems for these classes.

3. We also examined a number of issues relating basic properties of resource bounded quantum circuits, universal circuit families, and on the necessity of extra qubits (ancillae) used in their computations.

   - We have constructed a family of universal constant depth quantum circuits. These circuits can efficiently simulate any other family of constant depth quantum circuits.
   - We defined simple measurements of entanglement for small quantum systems which will allow us to prove lower bounds on the quantum circuit complexity of quantum circuits which compute simple combinatorial functions.
   - We found examples of natural functions needing additional ancillae in order to be efficiently computable.
   - We extended earlier upper and lower bounds on the computational capabilities of constant depth quantum circuits to other combinatorial problems and to circuits which have polylog depth.
   - We recently wrote of a 25 page survey paper which appeared this summer in the June issue of SIGACT News. It covered upper and lower bounds results for small depth quantum circuits. This work centers on the complexity of computing fanout, parity, mod functions and threshold gates using weaker gates such as CNOT and single qubit gates.

In general our research exposed differences between resource bounded quantum computation within various quantum models. Our work originates from the point of view of "classical" complexity, comparing and measuring the efficiency of quantum computation using the methods of complexity theory. A second focus and outgrowth of this and past work is the creation of efficient quantum circuit algorithms, in the form of quantum circuits for specific problems and functions. In particular we have studied constant depth quantum circuit classes constructed from limited, simple universal sets of gates, and quantum analogs of classical universal complexity classes such as NC, AC and ACC. Our goal is to measure and classify the complexity of problems solvable by small-depth quantum circuits and resource bounded quantum algorithms.

Our work then tells us what what circuit elements are necessary and which are sufficient to carry out specific natural quantum computations. It provides metrics which quantify the power and the limits of the various quantum circuit implementations. This research also impacts quantum algorithms as we are designing small circuits which can be used to implement and to improve the efficiency of fundamental quantum computations.

The remainder of this report contains brief summaries of the different results we have obtained, and ends with a discussion of the education and outreach accomplishments we have achieved. The bibliography contains a list of papers supported by this project.

Understanding the Computational Power of Constant Depth Quantum Circuits

We have been working on extending our understanding of the power of small depth quantum circuits made from a few simple gates each of which take a small number (usually three or less) qubits as input. Such circuits matter as it seems apparent that for the foreseeable future all circuits which are implemented will be no more powerful than these. We have shown that, when such circuits are allowed to have fanout gates, then they are surprisingly more powerful than their classical analogs. On the other hand, we have recently shown that languages defined by constant depth quantum circuits composed only of single qubit and CNOT gates have differing computational power depending on the accuracy demanded of the circuit computation which are used to decide membership in the language. And we have proved that constant depth circuits with single qubit and Toffoli gates cannot be exactly simulated by those with only single qubit and CNOT gates.

The "fanout problem" concerns the capability to unitarily provide the output of a gate to multiple other gates in a circuit. This relates to quantum circuit complexity and quantum data transmission. The fanout capability is available "for free" to classical circuits, and it is assumed to be available, as a unitary "controlled-fanout" gate. (Note that it is really only classical bits that are being fanned out here, the no-cloning theorem does not allow fanout of qubits, and the unitary extension of this function does not fanout arbitrary qubits.) It will be difficult to build efficient, that is constant depth, quantum circuits for many natural problems if efficient fanout is not possible. We have made recent progress in determining whether fanout is unavoidable in this setting or whether it can be circumvented by some new quantum circuit construction. We believe this is not possible in general, and that arbitrary fanout cannot be done by a constant depth circuit family using only single qubit and Toffoli gates. We have proved that fanout cannot be done by some specific, limited families of such gates.

One paper, “Quantum Lower Bounds for Fanout,” appeared in 2005 in the Journal of Quantum Information and Computation. This work, by Fang, Fenner, Green, Homer and Zhang, studies new lower bounds for constant depth quantum circuits constructed from a limited, though still universal, set of gates. The main results are that parity (and equivalently fanout) requires log depth circuits in two separate cases. First, log depth is necessary when the circuits are composed of any single qubit and cnot gates (or gates come from any finite set of 2 qubit gates). Second, log depth is still needed when the circuits are composed of single qubit and extended Toffoli gates (generalized CNOT gates of arbitrary arity), and when they are limited to only constantly many ancillae. (Ancillae are auxiliary qubits which provide extra work space for the circuit to carry out its computation.) Under this constraint, this bound is close to optimal. In the case of a non-constant number of ancillae, we give a tradeoff between the number of ancillae used in the computation and the required depth. We are currently working on trying to extend this lower bound to a polynomial number of ancillae and also exploring the necessity and power of ancillae for other central computations using quantum circuits.

To summarize, this work provides a way of building simple circuit modules useful for the construction of circuits for interesting combinatorial functions, and gives a simplification of the circuits needed to carry out current algorithms. We are currently working on finding constant depth quantum circuits that yield more efficient algorithms using smaller and less complex circuits and circuit elements.

The Power of Ancillae in Efficient Quantum Computation

Our work in this area shows that, for certain simple computations, there is a strict trade-off between the number of steps of the computation and the number of qubits in the quantum circuit carrying out the computation. The question of whether more than sublinear many ancillae would result in the possibility of fanout being computed in constant depth remains open, though we conjecture that additional ancillae do not help in this case. It arises from the fact that the proof of the lower bound for fanout, using only single qubit and Toffoli gates, is only known to hold in the presence of few ancillae highlights the issue of ancillae in constant depth quantum computation. The underlying issue is whether and when quantum computers require additional qubits (and how many are needed) to carry out basic computations is of considerable interest to theorists and practitioners alike.

We know that functions exist for which additional ancillae do help and make the difference between constant and non-constant circuit depth. Let + denote the “exclusive or” operation. Consider the function which takes as input n qubits $(x_1, x_2, ..., x_n)$ and which outputs $(x_1, x_1 + x_2, x_1 + x_2 + x_3, x_2 + x_3 + x_4, ..., x_{(n-2)} + x_{(n-1)} + x_n)$. We prove that this and related function cannot be computed by a constant depth quantum circuit but it can be efficiently computed if linearly many extra qubits are allowed in the quantum system. More precisely, using CNOT and single qubit gates, this function requires a log n depth quantum circuit to compute. We also prove that it can be computed by a circuit of depth (log n)(log n).

In fact there are functions F acting on n qubits for which we can prove:
(i) F takes log n depth to compute without ancillae
(ii) F can be computed in depth $(logn)^2$ without ancillae
(iii) F can be computed in constant depth **with n ancillae**. With fewer ancillae there is a trade-off between the number of ancillae used and the depth of the circuits needed to compute F. For example, with n ancillae the computation of F can be done in depth 3, with n/2 ancillae the depth is 4, etc. It is worth noting that these computations cannot be done cleanly.

Using Entanglement Measures to prove Lower Bounds on Quantum Computation

In research not yet fully completed, we have developed a new, limited measure of entanglement in a quantum state. This measure is weak in sense that it does not fully classify the degree of entanglement of a state (a more computationally difficult problem). Rather it allows us to algebraically analyze a pure quantum state and to effectively determine whether the state can be factored into the tensor product of two or more pure states. Our aim is to use our measure to achieve separations and lower bounds for quantum circuit classes. For example, we can analyze and compare the maximum amount of possible entanglement of unentangled pure states after application of fanout gates and single qubit gates versus the same measure after application of Toffoli gates and single qubit gates. By showing that our measure differs on the states reached after these two transformations of the same state, we hope to be able to prove that finite depth circuits of Toffoli and single qubit gates cannot be used to compute fanout, this giving a new lower bound proof for the power of fanout gates in quantum circuits. This is a first step in developing a new approach to proving lower bounds for different classes of quantum circuits and for better understanding the computational power of these circuits.

Upper Bounds and Simulations of Constant Depth Quantum Circuits

We have recently examined whether languages defined by constant depth quantum circuits without fanout gates have differing computational power depending on the accuracy demanded of the circuit computation which are used to decide the language. In the paper, "Bounds on the power of constant-depth quantum circuits," by Fenner, Green, Homer and Zhang, (in Proceedings of the 15th International Symposium on Fundamentals of Computation Theory, Luebeck, Germany, August 2005. Springer LNCS 3623, pages 44-55, and quant-ph/0312209) upper bounds on constant depth circuit classes are considered. We study QNC^0, the class of constant depth circuit families built from CNOT and single qubit gates. (Think of it this way. A circuit family is an infinite collection of circuits, C_n, which is designed to carry out a computation on problem inputs of any size. The circuit C_n is the one which does this for inputs of size n, typically n qubits. The circuit family being constant depth means there is a fixed constant k such that each circuit in the family has depth no more than k.)

The class $EQNC^0$ is the constant-depth analog of the class EQP. (EQP is the class of problems solvable in polynomial time by exact quantum algorithms, those which are correct with probability 1.) $EQNC^0$ consists of those languages L such that there is a (uniformly defined) circuit family in QNC^0 such that which decides membership of strings in L with probability 1. Similarly $NQNC^0$ ($BQNC^0$) languages are those where elements of L are those which are accepted by the circuit with positive probability (with probability $> 2/3$).

In our paper it is shown that, if a language is recognized within certain small error bounds by a QNC^0 circuit family, then it is computable in (classical) polynomial time. In particular, our results imply $EQNC^0$ is contained in P. On the other hand, we adapt and extend ideas of Terhal and DiVincenzo (quant-ph/0205133), regarding teleportation as a computation resource, to show that, for any family F of quantum gates including Hadamard and CNOT gates, computing the acceptance probabilities of depth-five circuits over F is just as hard as computing these probabilities exactly for circuits over F. In particular, this implies that $NQNC^0$ is hard for the polynomial time hierarchy, where $NQNC^0$ is the constant-depth analog of the class NQP. (NQP is the class of computational problems which can be decided by a polynomial time quantum algorithm, where a problem instance is accepted if the algorithm on that input instance has positive acceptance probability.) Hence there is a great difference in the power of QNC^0 circuits depending on the reliability/accuracy with which they are required to carry out their computations. We have also carried out related work (quant-ph/0106017 and quant-ph/0002057, with Moore and Pollett) which compares the power of different unitary gates in constant depth quantum circuits in simulating particular fundamental combinatorial functions. In particular, using constant depth quantum circuits which are allowed to have fanout gates, (and related work which has followed, principally by Hoyer, Spalek, Watrous and Cleve) has some strong consequences for quantum algorithms and the possibility of their having efficient implementations. In particular we now know the following constructions,

- the parity gate (and any other mod gate) can be built with a small circuit composed only of Toffoli, fanout, and single-qubit gates, and as well fanout can be built from parity.

- threshold gates can be similarly constructed, proving that integer division can be done with these circuits more efficiently than in classical computation.

- phase estimation can be done with small circuit families, showing that the quantum content of strong quantum algorithms like Shor's algorithm can be done with smaller and simpler circuits than had previously been thought possible.

This work provides a way of building simple circuit modules useful for the construction of quantum algorithms, and gives a simplification of the circuits needed to carry out current algorithms. We are currently working on finding constant depth quantum circuits that yield more efficient algorithms using smaller and less complex circuits and circuit elements.

Universal Quantum Circuits

Our recent research in this area focuses on constructing universal circuits for natural classes of quantum circuits. Our first result exhibits a universal circuit family U for any constant-depth quantum circuit family composed only of CNOT, single qubit and fanout gates. The circuit family U is universal in the sense that any other constant-depth circuit family composed from the same gates can be efficiently and uniformly simulated by U.

The existence of such universal families of circuits for a class of circuits C has been extensively studied in classical circuit theory, and universal circuits have been shown to exist for many classes of classical circuits. Such universal circuits are fundamental and useful as they provide an example of a uniform family of circuits which, once constructed give a platform on which any other circuit in C can be implemented (a kind of "compiler" for C). Our work is the first example of a universal circuit for a significant class of quantum circuits.

We are working to extend our results in several directions. We hope to prove a similar result for circuits of greater depth. In particular for circuits in the classes AC^k and in NC^k, both with and without fanout. We would also like to know if our result for finite depth circuits with fanout can also be carried out when the fanout gate is not included in the basic set of gates.

Complexity Classes and Associated Problems

In previous work the quantum class NQP, defined by Adelman, DeMarrais and Huang, was shown to be equal to the classical complexity class $coC_{=}P$. We have extended and continued this research direction in two different ways. Both the original work and the new research here was done in collaboration with Steve Fenner.

The above result has been strengthened to include the circuit class $NQAC^0$ (with fanout). That is, we proved that the class $NQAC^0$ equals $coC_{=}P$. This answers an open question we posed in our earlier work with Moore and Pollett (and in fact disproves a conjecture put forward in that work). The proof draws on the main result in the recent paper "Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games" by Terhal and DeVincenzo (quant-ph/0205133) and subsumes our previous result regarding the strength of the class NQP.

The study of a number of variants of NP in the quantum setting has continued, together with research comparing these classes with central quantum classes. The class $\exists EQP$, a natural quantum analog of NP, has been considered. $\exists EQP$ is the collection of languages defined by the existence of a (classical) existential witness to an EQP computation. We proved that $\exists EQP$ is contained in NQP. We also considered the power of allowing the witness to the computation be a quantum state, rather than a classical string. Here we showed that nothing is gained with a quantum witness to an NQP computation and that the resulting languages were the same as NQP.

The study of a number of variants of NP in the quantum setting has continued, together with research comparing these classes with central quantum classes. The class $\exists EQP$, a natural quantum analog of NP, has been considered. $\exists EQP$ is the collection of languages defined by the existence of a (classical) existential witness to an EQP computation. We proved that $\exists EQP$ is contained in NQP. We also considered the power of allowing the witness to the computation be a quantum state, rather than a classical string. Here we showed that nothing is gained with a quantum witness to an NQP computation and that the resulting languages were the same as NQP. We also established the chain of inclusions, $EQP \subseteq \exists EQP \subseteq QMA(one - sided) \subseteq NQP$, and can show that all these containments are proper relative to an oracle.

Education

This project has supported 4 students. Seth Roby, a computer science undergraduate major, did his honor's project studying and implementing a simulation of Shor's algorithm for factoring. Natalia Luckyanova, a Master's student worked for about 6 months on this project, before deciding to switch her focus to a project I had in computational chemistry with two members of the chemistry department. She finished her MA work on this project and received her degree in May of 2006.

Maosen Fang began quantum computing research in April of 2002. He spent the first part of the year working on problems related to quantum fanout. This work resulted in his co-authorship of the paper "Quantum Lower Bounds for Fanout," discussed above. Maosen finished his MA work last year and continues his Ph.D. work in this area in his study of the open problems which remain, notably lower bounds for general QNC^k circuit families. He is jointly supervised by Fred Green and Steve Homer. A second Ph.D. student Debajyoti Bera, is approaching the end of his graduate training, working on universal circuits for small depth quantum computation, as well as for more general classes of efficiently computable quantum functions. This work raises questions concerning how adding resources such as time, space and additional qubits allow for more powerful and efficient quantum computation. Debajyoti has also considered questions such as whether there are problems computed by a circuit family of fixed constant depth k, but not by any family of depth < k. He is also considering the affect of allowing limited ancillae in these circuits. There are several interesting results and we are working on refining and strengthening them, and within the next year, completing his Ph.D thesis. Recently Debajyoti was a co-author of the survey paper we wrote with Fred Green for the June, 2007 SIGACT News.

Several of the results from this project were presented at seminars in Computer Science and in Computational Science at Boston University, SUNY at Buffalo, the University of Maryland, UMass Lowell, Northeastern University, Clark University, Heidelberg University, and at a number of national and international conferences.

In 2004, together with Professor Peter Gacs, Steve Homer organized and taught a graduate level quantum computing seminar. Attendees included six Boston University Ph.D. students and two faculty members from local universities. We anticipate that the seminar will be repeated next year. Steve Homer also organized the continuing Boston University Theory Seminar, which meet weekly during the school year, and at which some of these results were presented and discussed.

The following bibliography contains papers written with the support of this grant.

References

D. Bera, F. Green, and S. Homer, Sigact News, June 2007. vol 38, no 2, pages 35-50.

F. Green, A. Roy, and H. Straubing, Bounds on an exponential sum arising in Boolean circuit complexity, in Comptes Rendus 341(5) (2005), pp. 279-282.

M. Fang, S. Fenner, F. Green, S. Homer, and Y. Zhang, Quantum lower bounds for fanout, arXiv preprint quant-ph/0312208. In Quantum Information and Computation 6 (2006), pp. 46-57.

S. Fenner, F. Green, S. Homer, and Y. Zhang, Bounds on the power of constant-depth quantum circuits, arXiv preprint quant-ph/0312209. Appeared in Proceedings of Fundamentals of Computation Theory: 15th International Symposium, Lecture Notes in Computer Science 3623 (2005), pp. 44-55.

F. Green, The Correlation Between Parity and Quadratic Polynomials Mod 3, in 17th Annual IEEE Conference on Computational Complexity, IEEE Computer Society Press (2002), pp. 65 -72. Appeared in Journal of Computer and System Sciences 69 (2004) pp. 28 - 44.

F. Green, S. Homer, and C. Pollett, On the complexity of quantum ACC, Boston University CS Dept. preprint BUCS-TR-2000-003, and in arXiv.org, report quant-ph/0002057. In 15th Annual IEEE Conference on Computational Complexity, IEEE Computer Society Press, (2000), pp. 250 - 262. Combined/expanded version with authors F. Green, S. Homer, C. Moore, and C. Pollett, under the title "Counting, fanout and the complexity of quantum ACC," appeared in Quantum Information and Computation 2 (2002), pp. 35 - 65. See arXiv preprint quant-ph/0106017.

F. Green and R. Pruim, Relativized separation of EQP from P(NP), in Information Processing Letters, 80 (2001) pp. 257 - 260.

S. Homer, and L. Fortnow, A Brief History of Complexity Theory, Bulletin of the European Association for Theoretical Computer Science (80), June 2003, pages 95-133. Presented at IEEE Conf. On Complexity Theory, Montreal, May, 2002.